Office of Information Security Newsletter

April 2007
Volume 2 Issue 3

INSIDE THIS ISSUE

Safeguarding Your Data

How do you safeguard sensitive/confidential data? The manner of protection often depends on what kind of data you are safeguarding, how important or sensitive it is to you, to your organization or your customers.

Types of data

Data can be defined, or classified, with labels such as public, personal, sensitive, confidential, secret, top-secret, or other categories. The more valuable or sensitive the data, the more it needs to be protected. By classifying the data you handle you are performing the first step of protection – by knowing what your data is you can then implement specific kinds of controls for that data.

The following tips will help you become aware of how to protect data both at work and at home.

Protect the Data

- **Password-protect your access** – Use a strong password or pass-phrase to protect access to your data.
- **Identify where the data is stored** – Have specific places within your network or computer where you store sensitive/confidential data. Those network shares, hard drives, servers, or system folders can then have specific protection methods used to keep them more secure.
- **Limit transportation and transmission of data** – Refrain from transporting or transmitting sensitive/confidential data if you don't need to do so. For example, don't allow or sensitive/confidential data to be sent via email or removed on a USB stick unless there is a clear need. When you do transport or transmit it, ensure that it has an appropriate level of security.
- **Limit physical access** - Whenever possible, store sensitive/confidential data on devices that are physically secured. Allow only authorized individuals access to those devices, and monitor access to those devices whenever possible.
- **Encrypt stored sensitive/confidential data** – Whenever possible, encrypt stored sensitive/confidential data, whether it is being permanently or temporarily stored. This can help prevent unintended disclosure even if your system has been compromised. *Only use approved encryption services.*

Cyber-Security
is
Everyone's
Responsibility

To find helpful links visit the OIS website at

http://infosec.nv.gov

Protecting Portable Devices

We've all read about lost or stolen portable devices containing confidential or sensitive information. Even if there isn't any sensitive or confidential customer information on your portable device, think of the other proprietary information that could be at risk: passwords, emails, contact information, etc.
Below are tips to help you secure and protect your portable device.

Steps to take before you leave the office

- **Password-protect your portable device** - Make sure that you have to enter a strong password to log in to your device. If possible use a "power-on" password. This prevents someone from booting up your laptop with a different Operating System on a CD, floppy disk, or flash drive.
- **Be sure all critical information is backed up** - Portable devices should not be the only place important information is stored.
- **Remove information that is not needed** - Don't carry around sensitive and personal information on your laptop or other portable device that is not necessary to you or your work.
- **Store your portable devices securely** - When not in use, store portable devices out of sight and, whenever possible, in a locked drawer or file cabinet.
- **Encrypt files or the full disk** - By encrypting files or using full disk encryption, you reduce the risk of unauthorized individuals viewing sensitive data.

Steps to take when traveling

- **When traveling by car -** If it is necessary to leave a portable device in a car, lock it in the trunk or other location where it is out of sight. Never leave electronic devices in cars for extended periods during either very hot or very cold weather. Never leave the vehicle unlocked when unattended, even for a minute. Do not leave the portable device in the vehicle overnight.
- **When traveling by air or rail** - Always keep your portable device with you or as carry-on luggage. Watch your device carefully as it goes through the screening process - this is an opportune time for a thief to take it. Make sure you have your portable device with you each time you board or disembark.
- **At conferences and trade shows** - Be especially wary at conferences, large meetings and trade shows. These are common venues for thieves.
- **In the hotel room** - If a room safe is available, lock the device with other valuables in the safe. If it does not fit in the room safe, ask the hotel staff for the use of the hotel safe. If this is not practicable, store the portable device out of sight when you leave the room.

What should you do if your laptop or other portable device is lost or stolen?

Report the loss or theft to the appropriate authorities as soon as possible. These parties may include representatives from the following:

- Local law enforcement agencies
- Hotel or conference staff
- Airport or other transportation security offices
- Your organization's information security officer or Help Desk.
  They can then inform the appropriate parties to help protect any services that may be at risk.